SSL چیست و چرا استفاده از آن مهم است؟

نویسنده: مهران منصوری فر

آیا می‌دانید https:// چیست و چه تفاوتی با http:// دارد؟ آیا می‌دانید که SSL چیست؟؟ در این مطلب به زبان ساده شما را با این مفاهیم امنیتی، اهمیت و مزیت آن‌ها و همچنین چگونگی دریافت گواهی SSL آشنا خواهیم کرد.

آیا تابه‌حال به این نکته دقت کرده‌اید که آدرس بعضی از وب‌سایت‌ها با http:// و آدرس برخی دیگر با https:// شروع می‌شود؟ چنانچه کاربر مرورگر کروم باشید و به سراغ وب‌سایت‌هایی رفته باشید که حاوی فرم یا فرم‌هایی برای درج اطلاعات هستند (مثلاً فرم پرداخت) این موضوع بیشتر به چشمتان خورده است.
اما این s اضافی از کجا می‌آید و چه معنایی دارد؟
به زبان ساده، آن s اضافی به این معنی است که وب‌سایت مزبور امن و رمزگذاری شده است و اطلاعاتی که با آن مبادله می‌کنید فقط بین خودتان و همان وب‌سایت باقی خواهد ماند. فناوری پشتوانه آن s کوچک با نام SSL شناخته می‌شود که مخفف عبارت Secure Sockets Layer به معنی «لایه سوکت های امن» است. اما آیا دقیقا می‌دانید که SSL چیست؟
در این مطلب قصد داریم که مبحث SSL را بیشتر باز کنیم، ببینیم که این قابلیت امنیتی چه منفعتی دارد و با نحوه دریافت آن نیز آشنا شویم.

SSL چیست؟

در ابتدا به سراغ تعریف وب‌سایت SSL.com از SSL می‌رویم:
SSL یک فناوری امنیتی استاندارد برای برقراری یک پیوند رمزگذاری شده بین یک سرور و یک مرورگر است. این پیوند امن، محرمانه باقی ماندن تمامی داده‌هایی که بین سرور و مرورگر رد و بدل می‌شوند را تضمین می‌کند.
اجازه بدهید که این تعریف را بازتر کنیم.
هنگامی‌که وارد صفحه‌ای می‌شوید که حاوی یک فرم است، بعد از آنکه فرم مزبور را تکمیل کردید و دکمه ارسال را فشردید، اگر آن صفحه گواهی SSL نداشته باشد تمامی اطلاعاتی که در فرم مزبور وارد کرده‌اید توسط هکرها قابل مشاهده خواهد بود.
این اطلاعات می‌تواند هر چیزی باشد؛ از اطلاعات تراکنش‌های بانکی گرفته تا اطلاعات خصوصی مهمی که برای ثبت نام در سرویس‌های مختلف وارد می‌کنید. هکرها به این سرقت اطلاعات، «حمله مرد میانی» (به انگلیسی man-in-the-middle attack) می‌گویند. حمله مزبور را از روش‌های مختلفی می‌توان انجام داد، اما یکی از رایج‌ترین روش‌های آن از این قرار است: هکر یک برنامه کم حجم و غیرقابل شناسایی جاسوسی را بر روی سروری که از وب‌سایت مورد نظر میزبانی می‌کند قرار می‌دهد. این برنامه در پس زمینه منتظر می‌ماند تا بازدیدکننده‌ای وارد یک وب‌سایت شود و درج اطلاعات در یکی از فرم‌های آن را آغاز کند؛ برنامه ذکرشده با درج اطلاعات فعال می‌شود، اطلاعات مربوطه را ثبت می‌کند و آن‌ها را برای هکر می‌فرستد؛ داستان ترسناکی که دیگر مشاهده آن فقط به فیلم‌های علمی-تخیلی محدود نمی‌شود.
اما هنگامی‌که از وب‌سایتی دیدن می‌کنید که با SSL رمزگذاری شده، مرورگر شما گواهینامه SSL را بررسی می‌کند و یک ارتباط واقعاً امن را بین مرورگر و سرور برقرار می‌کند. در این حالت هیچ‌کس به‌جز شما و وب‌سایتی که اطلاعاتتان را برای آن ارسال می‌کنید نمی‌تواند به آنچه که در مرورگر خود تایپ می‌کنید دسترسی داشته باشد یا آن اطلاعات را به هر نحوی مشاهده کند. امروزه برخلاف گذشته، سرعت این ارتباط بالا بوده و حتی از برخی از وب‌سایت‌های بدون SSL نیز سریع‌تر است.

بنابراین تمام کاری که کاربر برای امن کردن ارتباط خود باید انجام بدهد این است که از وب‌سایت‌هایی استفاده کند که آدرس آن‌ها با https:// شروع می‌شود و گواهینامه SSL معتبر دارند. از این طریق، ارتباط کاربر با سرور رمزگذاری می‌شود و کاملاً امنیت پیدا می‌کند.

بیشتر بدانید: CDN چیست و چه تاثیری در سئو و امنیت سایت دارد؟

کروم و SSL

امنیت برای گوگل به‌عنوان یک غول جستجو و شرکتی که برای بقای خود به‌شدت به اینترنت وابسته است اهمیت فراوانی دارد؛ در نتیجه، این شرکت از نسخه ۶۲ مرورگر خود موسوم به «کروم» برای همه وب‌سایت‌هایی که بدون داشتن گواهینامه SSL از هر نوعی از فرم‌های ثبت اطلاعات استفاده می‌کنند، هشداری را مبنی بر ناامن بودن آن‌ها برای کاربر نمایش می‌دهد. توجه داشته باشید که بر طبق نتایج یک تحقیق، ۸۵ درصد از کاربران به بازدید از وب‌سایتی که امن نیست ادامه نمی‌دهند.

بنابراین باید دقت کنید که اگر در وب‌سایتتان از هر نوعی از فرم استفاده می‌کنید، حتی فرم ثبت ایمیل یا فرم جستجو، باید گواهی SSL معتبر داشته باشید تا مرورگر کروم وب‌سایت شما را بدون مشکل برای کاربر نمایش بدهد. نکته دیگری که باید به آن توجه داشته باشید این است که اگر بخشی از محتوای وب‌سایتتان، مثلاً تصاویر یا ویدئوهای آن را در آدرس یا پلتفرم دیگری بارگذاری کرده‌اید، آن منبع نیز باید گواهی SSL داشته باشد و گواهی وب‌سایت شما قابل تسری به آن نیست.

به‌طورکلی، فارغ از اینکه در کدام صفحه یا صفحات وب‌سایت شما فرم وجود دارد، بهتر است که گواهی SSL را برای کل سایتتان فعال کنید؛ چرا که وجود این اعتبارنامه می‌تواند برای سئوی شما نیز مزایایی داشته باشد که در قسمت بعد به شرح آن می‌پردازیم.

مزایای SSL

امروزه وجود SSL برای هر وب‌سایت و وبلاگ و به‌خصوص وب‌سایت‌های شرکتی از حالت گزینه درآمده و به یک ضرورت تبدیل شده است؛ چرا که مزایای غیرقابل انکاری دارد که اهمیت آن‌ها بر کسی پوشیده نیست، از جمله:

۱. SSL از اطلاعات محافظت می‌کند

کار اصلی گواهی SSL حفاظت از اطلاعاتی است که در ارتباط بین کاربر با سرور رد و بدل می‌شود. با نصب SSL هر بیت از داده‌ها رمزگذاری خواهد شد؛ به زبان ساده، اطلاعات قفل می‌شوند و کلید بازگشایی این قفل فقط در اختیار دریافت کننده مورد نظر قرار دارد.

SSL علاوه بر محافظت از اطلاعات حساسی مانند رمزهای عبور و اطلاعات کارت‌های بانکی، در مقابله با لشکر هکرها و خرابکاران اینترنتی نیز به شما کمک می‌کند. ازآنجایی‌که داده‌ها توسط SSL به یک فرمت غیرقابل خواندن تبدیل می‌شوند، مهارت‌های هکرها در برابر فناوری رمزگذاری بی‌همتای SSL به یک شمشیر بی لبه می‌ماند.

۲. SSL هویت شما را تأیید می‌کند

دومین وظیفه اصلی گواهی SSL، تأیید اعتبار وب‌سایت است. تردیدی وجود ندارد که حجم تقلب و کلاه‌برداری در اینترنت به‌طور روزافزونی در حال افزایش است و بسیاری از مردم چه از نظر مالی و چه در ابعاد دیگر، با استفاده کردن از وب‌سایت‌های تقلبی متحمل خسارت‌های جبران‌ناپذیری شده و می‌شوند.
هنگامی‌که می‌خواهید گواهی SSL نصب کنید باید وارد یک فرآیند اعتبارسنجی شوید که طی آن، بسته به نوع گواهینامه، هویت شما و سازمان متبوعتان سنجیده می‌شود. پس از تأیید اعتبار، وب‌سایت شما گواهینامه‌ای دریافت می‌کند که کاربر با توجه به آن می‌تواند مطمئن باشد که با همان کسی در تعامل است که باید باشد.
البته توجه داشته باشید که همان‌طور که ذکر شد، هویت سنجی بسته به نوع گواهینامه‌ای که به دنبال دریافت آن هستید متفاوت خواهد بود؛ به‌عنوان مثال، برخی از صادرکنندگان گواهینامه‌های SSL، از جمله وب‌سایت‌های رایگانی مانند Let’s Encrypt زیاد در این رابطه متعه به خشخاش نمی‌گذارند. لذا به عنوان صاحب یک کسب‌وکار معتبر پیشنهاد می‌شود که از گواهینامه‌های معتبرتری استفاده کنید که هویت شما را نیز تأیید می‌کنند.

۳. SSL پیش‌نیاز اصلی دریافت نماد اعتماد دوستاره است

یکی از روش‌های شناخته‌شده برای تأیید اعتبار صاحبان کسب‌وکارها و محل کارشان داشتن نماد اعتماد است. در واقع، امروزه اگر وب‌سایت کسب‌وکار شما نماد اعتماد نداشته باشد هیچ‌کس به آن اعتماد نخواهد کرد. در حال حاضر، نماد اعتماد در دو سطح یک ستاره و دوستاره اعطا می‌شود که تفاوت عمده این دو در ضرورت وجود یک گواهی SSL معتبر یک‌ساله برای دریافت نماد دوستاره است. دقت داشته باشید که با گواهی‌های رایگان نمی‌توانید نماد دوستاره دریافت کنید.

۴. SSL باعث تقویت حس اعتماد مشتری می‌شود

امروزه مشتریانی که حتی اندکی از دنیای وب و مخاطرات آن آگاهند ابداً به

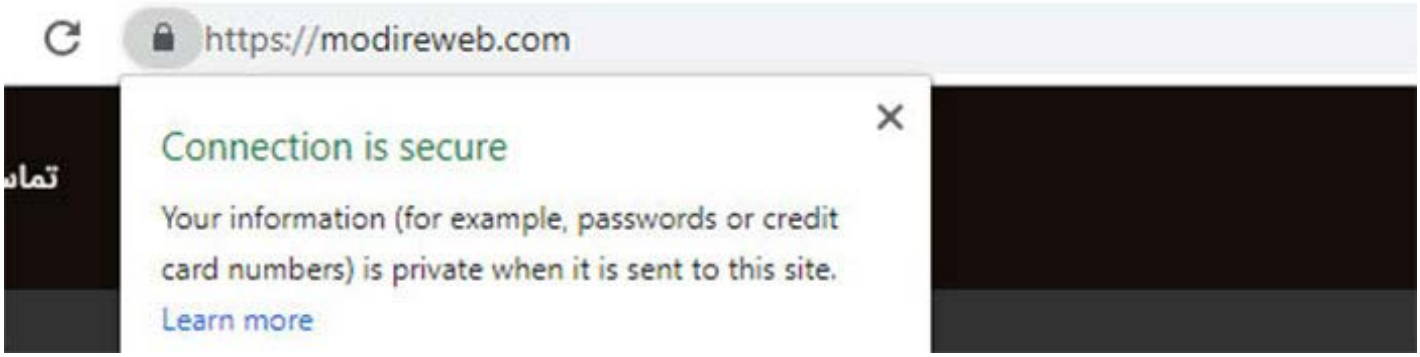
وب‌سایت‌هایی که گواهی SSL ندارند اعتماد نمی‌کنند؛ چرا که علاوه بر مشکلات مرتبط با سرقت و افشای اطلاعات شخصی و بانکی که پتانسیل روی دادن آن‌ها برای این‌گونه وب‌سایت‌ها وجود دارد، نداشتن گواهی SSL به نوعی به معنای بی‌مبالاتی صاحب وب‌سایت و کسب‌وکار مربوطه نیز خواهد بود. طبیعتاً با توجه به رقابتی که امروزه در دنیای کسب‌وکار موج می‌زند، کسی از فروشنده‌ای که برای امنیت کسب‌وکار و مشتریان خود اهمیتی قائل نیست خرید نخواهد کرد.

۵. SSL باعث بهبود رتبه شما در نتایج موتورهای جستجو می‌شود

آیا SSL برای سئو نیز مفید است؟ پاسخ به این سؤال مثبت است. علیرغم اینکه هدف از SSL ایمن‌سازی تبادل اطلاعات بین بازدیدکننده و وب‌سایت است، اما وجود گواهی SSL به‌عنوان یک امتیاز در مبحث سئو نیز محسوب می‌شود. بر طبق نتایج بررسی‌های تجربی انجام‌گرفته، یکی از مؤلفه‌های تأثیرگذار در الگوریتم رتبه‌بندی گوگل، وجود SSL است.

علاوه بر این، گوگل نیز رسماً اعلام کرده است که اگر دو وب‌سایت از همه نظر با هم برابر باشند، اما یکی از آن‌ها گواهی SSL داشته باشد، احتمالاً در نتایج جستجو برای آن نسبت به دیگری اولویت قائل خواهد شد. در نتیجه، فعال‌سازی SSL در وب‌سایت و برای تمامی محتواهای داخل و خارج از آن به نفع سئوی سایت خواهد بود.

تشخیص وجود SSL: چگونه متوجه شویم که یک وب‌سایت گواهی SSL دارد؟
هنگامی‌که به وب‌سایتی مراجعه می‌کنید که گواهی SSL دارد، نشانه‌های خاصی را در مرورگر خود مشاهده می‌کنید که آن را نسبت به وب‌سایت‌های فاقد SSL متمایز می‌سازند:
۱. در آدرس وب‌سایت به جای https ،//:http وجود دارد؛
۲. در کنار آدرس سایت یک علامت قفل مشاهده می‌کنید که با کلیک بر روی آن می‌توانید جزئیات گواهی SSL وب‌سایت را مشاهده کنید؛ مثلاً در مرورگر کروم چیزی شبیه به تصویر زیر را می‌بینید:



۳. گواهی SSL وب‌سایت نیز باید اعتبار داشته باشد. توجه داشته باشید که در برخی موارد گواهی SSL وب‌سایت می‌تواند به دلایلی مانند اتمام تاریخ انقضای آن از اعتبار افتاده باشد. در این حالت اگرچه آدرس وب‌سایت همچنان با https:// شروع می‌شود و حتی شاید در برخی از مرورگرها علامت قفل نیز حذف نشود، اما ارتباط شما با وب‌سایت مزبور رمزگذاری شده و امن نیست.
به منظور بررسی اعتبار گواهی SSL در مرورگر کروم، از منوی آن به more tools و سپس Developer Tools بروید. سپس زبانه Security را انتخاب کنید. در اینجا می‌توانید اطلاعات مربوط به اعتبار گواهینامه را مشاهده کنید. با

کلیک بر روی دکمه View certificate اطلاعات دقیق‌تر به همراه تاریخ اعتبار گواهی SSL در دسترس شما قرار خواهد گرفت. ضمناً با کلیک بر روی علامت قفل موجود در کنار آدرس سایت نیز معتبر بودن گواهی قابل مشاهده است؛ درصورتی‌که گواهی معتبر باشد در کنار کلمه Certificate کلمه valid درج شده است که با کلیک بر روی آن می‌توانید به همان پنجره View certificate دسترسی پیدا کنید.

بیشتر بخوانید: ۵ نکته جهت بهبود امنیت سایت

دریافت گواهی SSL: چگونه برای وب‌سایتمان گواهینامه SSL بگیریم؟

اولین قدم برای دریافت گواهی SSL، تعیین نوع گواهینامه‌ای است که به آن نیاز دارید. به‌عنوان مثال، اگر محتوای وب‌سایت خود را در پلتفرم‌های مختلفی قرار داده‌اید (در دامنه‌ها یا زیردامنه‌های مجزا) به گواهینامه‌های SSL متفاوتی نیاز خواهید داشت.

معمولاً ارائه‌دهندگان خدمات SSL سرویس‌های متنوعی را پیشنهاد می‌کنند که هر یک با نیازهای خاص وب‌سایت‌ها و شرکت‌های مختلفی تناسب دارد. عمده تفاوت این سرویس‌ها به میزان تضمین SSL و تعداد دامنه‌ها و زیردامنه‌هایی مربوط می‌شود که توسط هر گواهی قابل پوشش است.

استفاده از گواهینامه‌های SSL استاندارد برای اغلب وب‌سایت‌ها کفایت خواهد کرد؛ اما برای شرکت‌هایی که در حوزه‌های تخصصی‌تر و قانونمندتری (از جمله امور مالی و بیمه) فعالیت می‌کنند بهتر است که دقت نظر بیشتری در رابطه با انتخاب گواهی مربوطه وجود داشته باشد.

هزینه خرید گواهینامه‌های SSL متفاوت است؛ به‌علاوه، گواهینامه‌های رایگان SSL نیز وجود دارند. یکی از وب‌سایت‌هایی که گواهی معتبر SSL رایگان ارائه می‌کند، وب‌سایت Let›s Encrypt است. توجه داشته باشید که معمولاً گواهینامه‌های رایگان هر ۹۰ روز باید مجدداً تمدید شوند؛ اما دوره تمدید اغلب گواهینامه‌های پولی یک یا دوساله است.

وردپرس و SSL: معرفی افزونه‌هایی برای نصب و مدیریت SSL در وردپرس

اگر برای مدیریت محتوای وب‌سایت خود از سیستم مدیریت محتوای وردپرس استفاده می‌کنید، افزونه‌های رایگان زیر می‌توانند در نصب و مدیریت SSL به شما کمک کنند:

- **Really Simple SSL**: این افزونه نصب گواهی SSL خریداری شده را آسان می‌کند.
- **Insecure Content Fixer**: معمولاً کار شما پس از خریداری و نصب گواهی SSL کاملاً تمام نمی‌شود. اگر وب‌سایتتان حاوی ارجاعاتی به آدرس‌های http باشد که از طریق کدهای استاتیک ایجاد شده‌اند، هیچ بعید نیست که برخی از فایل‌ها همچنان از طریق آدرس http در صفحه بارگذاری شوند. در اینصورت پس از بارگذاری صفحه در کنار آدرس آن یک علامت هشدار درج خواهد شد. این افزونه در پیدا کردن و رفع چنین مشکلاتی به شما کمک می‌کند.
- **WP Force SSL**: پس از آنکه گواهی را خریداری و نصب و مشکلات احتمالی را رفع و رجوع کردید، باید کاری کنید که کاربرانی که از لینک‌های حاوی http

استفاده می‌کنند نیز به آدرس https انتقال داده شوند. این افزونه کل ترافیکی که به سمت وب‌سایت شما می‌آید را به آدرس https آن ارجاع می‌دهد تا همه کاربران فقط از حالت امن وب‌سایت استفاده کنند.

حرف آخر

امروزه همه مردم و به‌خصوص کاربران اینترنت برای امنیت خود اهمیت خاصی قائل هستند. یکی از مؤثرترین موارد برای حفظ این امنیت در وب‌سایت‌ها، داشتن گواهی SSL است. وجود این گواهی علاوه بر تأمین امنیت کاربران و افزایش اعتبار و قابلیت اعتماد به شما برای تقویت و بهبود سئو نیز سودمند خواهد بود. بنابراین اگر هنوز وب‌سایت خود را به گواهی امنیتی SSL مجهز نکرده‌اید همین امروز آستین‌ها را بالا بزنید و با انتخاب یک سرویس‌دهنده معتبر، امنیت و اعتبار را به آن ارزانی کنید.